INFORMATION DISCLOSURE STATEMENT BY APPLICANT Form PTO-1449 (Modified) (Use several sheets if necessary)				COMPLETE IF KNOWN	
				Application Number	09/877,302
				Confirmation Number	9725
				Filing Date	June 8, 2001
				First Named Inventor	Hovav SHACHAM
				Group Art Unit	2136
				Examiner Name	PARTHASARATHY, P.
Sheet	1	of	2	Attorney Docket No.	36321-8006.US01

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.	U.S. Patent or Application NUMBER	Kind Code (if known)	Name of Patentee or Inventor of Cited Document	Date of Publication or Filing Date of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.	Foreign Patent or Application Office	NUMBER	Kind Code (if known)	Name of Patentee or Applicant of Cited Document	Date of Publication or Filing Date of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T
[signature]	1.	WO	01/03398		IBM Corp and IBM UK Limited	01/11/2001		

OTHER PRIOR ART-NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume issue number(s), publisher, city and/or country where published.	T
[signature]	2.	Netscape; "Netscape Proxy Server Administrator's Guide, Version 3.5 for Unix"; February 25, 1998; Retrieved from the Internet.	
[signature]	3.	"PKCS #1 v2.0 Amendment 1: Multi-Prime RSA," 2000	
[signature]	4.	"Security Protocols Overview (An RSA Data Security Brief)", RSA Data Security, 1999, http://www.comms.scitech.susx.ac.uk/fft/crypto/security_protocols.pdf, pages 1-4.	
[signature]	5.	Boneh, D., "Twenty Years of Attacks on the RSA Cyrptosystem," Notices of the AMS, Vol 46, No. 2, pp. 203-213, 1999	
[signature]	6.	Boneh, et al., "An Attack on RSA Given a Small Fraction of the Private Key Bits," ASIACRYPT '98, LNCS 1514, pp. 25-34, 1998	
[signature]	7.	Boneh, et al., "Cryptanalysis of RSA with Private Key d Less than $N^{0.292}$," (extended abstract), 1999	

EXAMINER	DATE CONSIDERED
PRAMILA PARTHASARATHY	June 01, 2005

*EXAMINER: Initial if reference considered, whether or not criteria is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to application(s).

INFORMATION DISCLOSURE STATEMENT BY APPLICANT Form PTO-1449 (Modified) (Use several sheets if necessary)				COMPLETE IF KNOWN	
				Application Number	09/877,302
				Confirmation Number	9725
				Filing Date	June 8, 2001
				First Named Inventor	Hovav SHACHAM
				Group Art Unit	2136
				Examiner Name	PARTHASARATHY, P.
Sheet	2	of	2	Attorney Docket No.	36321-8006.US01

OTHER PRIOR ART-NON PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume issue number(s), publisher, city and/or country where published.	T
	8.	Boneh, et al., "Efficient Generation of Shared RSA Keys," (extended abstract)	
	9.	Durfee, G., et al., "Cryptanalysis of the RSA Schemes with Short Secret Exponent from Asiacrypt '99," ASIACRYPT 2000, LNCS 1976, pp. 14-29, 2000	
	10.	Fiat, A. "Batch RSA," Springer-Verlag, 1998	
	11.	Großschädl, J., et al., "The Chinese Remainder Theorem and its Application in a High-Speed RSA Crypto Chip," 2000	
	12.	Immerman, N., "Homework 4 with Extensive Hints," 2000	
	13.	Menezes, A., et al., "Handbook of Applied Cryptography," 1996 CRC Press, pp. §8.2-8.3 and §14.5	
	14.	Oppliger, R.; "Authorization Methods for E-Commerce Applications"; 1999	
	15.	Shacham, H., et al., "Improving SSL Handsake Performance via Batching," Topics in Cryptology, pp. 28-43, 2001	
	16.	Shand, M., et al., "Fast Implementations of RSA Cryptography," 1993	
	17.	Sherif, M.H., et al., "SET and SSL: Electronic Payments on the Internet," IEEE, pp. 353-358 (1998)	
	18.	Stallings, W., "IP Security," Network Security Essentials, Applications and Standards, Chapters 6 and 7, pp. 162-223, 2000	
	19.	Takagi, T., "Fast RSA-Type Cryptosystem Modulo $p^k q$," 1998	
	20.	Takagi, T., "Fast RSA-Type Cryptosystems Using N-Adic Expansion," Advances in Technology – CRYPTO '97, LNCS 1294, pp. 372-384, 1997	
	21.	Wiener, M., "Cryptanalysis of Short RSA Secret Exponents," 1989	

EXAMINER	DATE CONSIDERED
PRAMILA PARTHASARATHY	June 01, 2005

*EXAMINER: Initial if reference considered, whether or not criteria is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to application(s).